Secure IOT Infrastructure Based Smart City Services Using Augmented Reality Techniques

Dr.Mallikarjunaswamy S, Dr.Nataraj K R, Dr. Komala M, Balachandra P

Abstract— **Augmented reality finds application in the service of a smart in public transport domain. This paper presents the above mentioned application deployed in Bengaluru. Important details such as arrival time of bus its routes, etc. can be accessed by the citizens easily in an efficient manner using AR technology along with smart phones. Triggering of Augmented Reality information is achieved by markers used to mark geo-location and image. The data is sent along a secured IOT infrastructure. A secured CoAP software protocol is used by the bus-mounted IOT devices to transfer the data to the cloud servers. A solution end-to-end description is presented in this paper gives complete information about overall system setup, user's experiences and security of overall system, which focuses on lightweight encryption used in IOT devices.**

Index Terms— **Intelligent Transport system, Smart farming, Augmented Reality Information, Smart City, Smart transport, Internet Protocol Security (IPsec),Secure IOT, Information and communications technology (ICT), Secure CoAP.**

I. INTRODUCTION

With increase in population, the number of people living in cities is also increasing. The number of people migrating to cities is also increasing, because of industrialization and other job opportunities. Improvement in services available in the cities the quality of services is most important to meet the increasing need. Attaining higher energy efficiencies from existing equipment's, automating existing systems is very important. Expectation of data at finger-tip is increasing and services have to meet people's demand. All service –oriented complex systems are now depending on ICT for upgradation some of these system include public utility public transport, public administration and health. An AR powered smart transportation service which aims in improvement of quality of public transportation services to passengers, profit to stockholders is presented is this paper.

II. AUGMENTED REALITY

Augmented Reality Technology aims in replacing real world view with data generated from computer (Ex: videos, audio, photos, GPS data).Augmentation process starts as soon as AR markers are deleted. On the basis of detected marker, the appropriate AR content is presented. Markers can be any detected real time images, tracked real time images and pre-defines images. These images can be obtained using images processing algorithms. Certain GPS locations, orientations of camera capturing live video stream can be used as markers.

AR technologies has wide applications such as military, medical, industrial, commercial and entertainment sectors. AR technologies comprises camera location sensors, image processing engine.

A smartphone is one of the main devices which support AR application. This smartphone has CPU, GPS and RAM which forms a complete system capable of algorithm executing image processing.

III. AUGMENTED REALITY TECHNOLOGY IN SMART CITIES

Currently, application of augmented reality in city services is not available. [1] refers to application of smart Santander AR in the field of weather forecast report, bike- rental service, public-buses information, real time access to beach and traffic , generation of unique ecosystem for citizen has been enabled . Santander city is considered and information of about 2700 places is considered in the application. The places are categorized as museums, art galleries, monuments, parks, gardens, public buses, taxis, parking places etc. public transport incorporates information about bus stop locations and passing of bus lines. No real time information of buses in included. [2] Has a project that mainly aims in validation of methodologies of open and user-driven innovation.

Augmented Reality technology finds important application in public transport. A secure system built using this technology helps public as well as the management .Also, identification of security issues and potential threats is done and suitable solutions are devised to enable specific issues like data security and data privacy to be addressed, thereby reducing commercialization problems.

IV. DESCRIPTION OF SERVICES IN PUBLIC TRANSPORT

The proposed system aims in improving the public transport network management in Bengaluru city, initially starting from bus transport network. Implementation of such system benefits both passengers and stockholders. An overview of the above system is shown in figure 1, which indicates the main components of Augmented Reality technology based public intelligent transport service buses have fleet management devices mounted on them to track their real time location, such devices communicate with cloud infrastructure at backend on a continuous basis.

The system contains the following components:

Manuscript received Dec 14, 2016

Dr.Mallikarjunaswamy S, Asso.Prof, SJB Institute of Technology Bengaluru-60
Dr.Nataraj K R, Prof & HOD, SJB Institute of Technology Bengaluru-60
Dr. Komala M, Asso.Prof, SJB Institute of Technology Bengaluru-60
Balachandra P, Asst.Prof, SJB Institute of Technology Bengaluru-60

1. With the help of a dedicated application in mobile/ smartphone, the passengers interact with the system (Cloud Infrastructure at back end)
2. Augmented Reality markers in bus stops either in the form of QR code, image code or bar code.
3. An operator of Cell-phone network who provides a LTE/3G/GPRS to transfer data from mobile and fleet managing devices to the server (Cloud Infrastructure at back-end).
4. Buses, which are equipped with fleet management devices that track the real-time location and communicate having a cloud platform at the back end
5. Web portals providing a safe access of entire system for users/ passengers as well as the stakeholders. It also ensures report generated, data of bus location, creation of AR data are done in secure manner.
6. Core function of the system is carried out by back end cloud platform which include communication, generation and handling of AR content, Web application and web server.

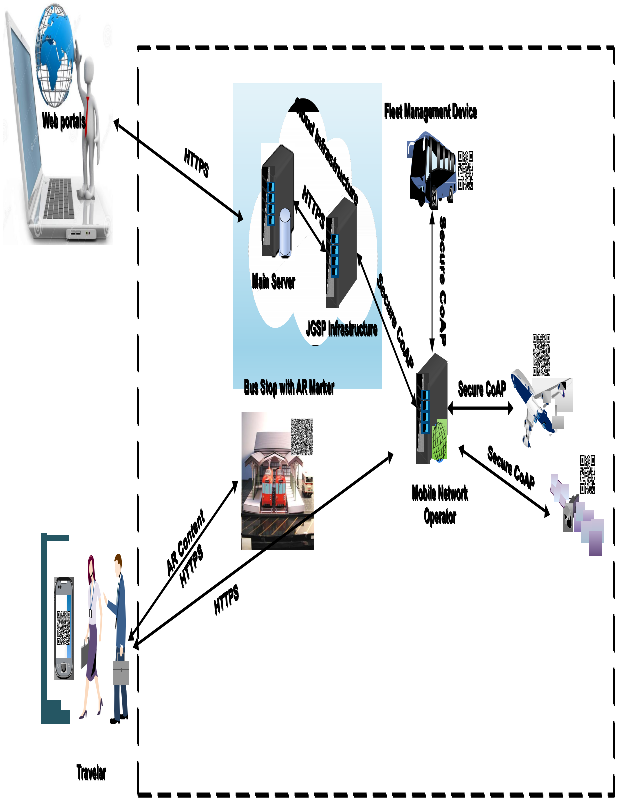

Figure 1: Overview of public transport system powered by Augmented Reality Technology.

The passengers of public transport (buses in this case) will be able to know the bus arrival time, using their smartphone, application and Augmented Reality markers at bus stops. Details about suitable route for a specific destination is also available based on criteria specified by the users a quickest like cheapest and shortest.The Augmented Reality view of a bus stop which has a QR code that displays arriving time of the bus is shown in figure 2. In addition to above mentioned features the system also provides the following services used by passengers and stakeholders:

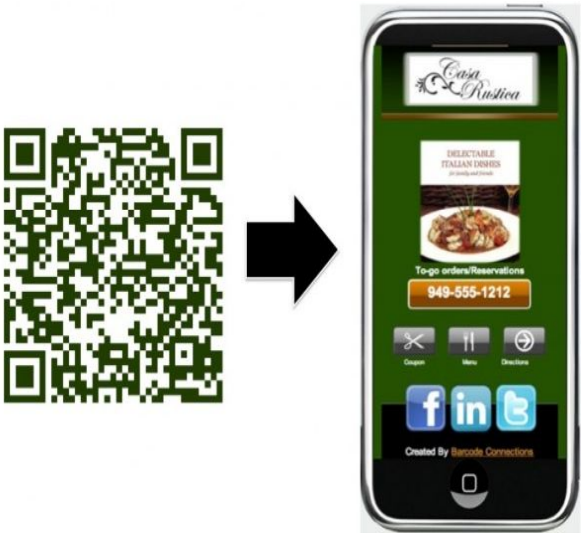
Casa Rustica
DELECTABLE ITALIAN DISHES
To-go orders/Reservations
949-555-1212
Coupon
Menu
Directions
Created By Barcode Connections

Figure 2: Experience by the user while using AR smartphone application.

- Current demand of passengers in specific routes -This feature is based upon calculation done using information received from smartphone application in which the transportation routes are specified by passengers.
- Current traffic conditions in specific routes – This feature is implemented based on the data obtained by the fleet management devices mounted on buses. This data can be obtained by knowing in time of current travel and expected travel of the bus along a gives route.
- Current location of passengers- Expected time of arrival of bus at certain stop or location – calculated using data of current location of bus and current traffic conditions.

Figure 3 shows the architecture of proposed system. The system contains passenger's smartphone, cloud infrastructure, devices for fleet management. The model aims to design architectural foundations of future. Internal of Things (IOT), which allows integration of heterogeneous IOT technologies into one single coherent architecture.An android platform is used to implement the smartphone AR application. Further this can be available on IOS. Qualcomm's vuforia SDK method is adopted for working of Augmented Reality market detection engine [3]. The engine is used for processing live video clips obtained from mobile's camera. Mobile application has integration SDK and detects AR marker, currently in QR code form which is located at the bus stop as shown in figure 2 information frame –to-frame basis is obtained by AR SDK and AR marker is identified on this marker position detection is done for each frame captured and hence smooth tracking and overlaying of AR content performed. Defining location based marker on the other hand helps to display AR information once the passenger reaches certain location.

Detection of image or location based markers enables usage of appropriate UI to present required information like bus arrival times route selection and other such details communication engine enables communication with cloud infrastructure , by using services from web. Security component is used to implement security aspects of smartphone application which includes encryption, decryption, and user authentication.

All security components are contained in cloud infrastructure. Fleet management devices, Smartphone users and other users and other users of system is done by the communication engine through secure channels. AR content engine provides access to the AR content and also enables city authorities and bus Service Company in creation of dynamic AR content which will be given to all passengers.

The device that calculated time of bus arrival and its route makes use of data from fleet management device and passengers routing plans respectively. Real time location of bus, bus step distance, current estimation of traffic conditions, and knowledge of arrival times at particular hour of the day are used to calculate bus arrival time.

Implementation of web server and web applications is done to allow accessing of cloud infrastructure by other users.

GPS/GPRS modem is the core component of fleet management device, and gives location of GPS is addition to communication like to Global System for Mobile (GSM) network operator. Execution of program code is done by embedded microcontroller and flash memory which provide limited processing capabilities .Lightweight encryption and decryption algorithm is provided by security engine component which ensures safe transfer of data to cloud infrastructure through a communication system engine. The Data handling component perform tasks like processing of data, its storage, parsing and packing tasks.

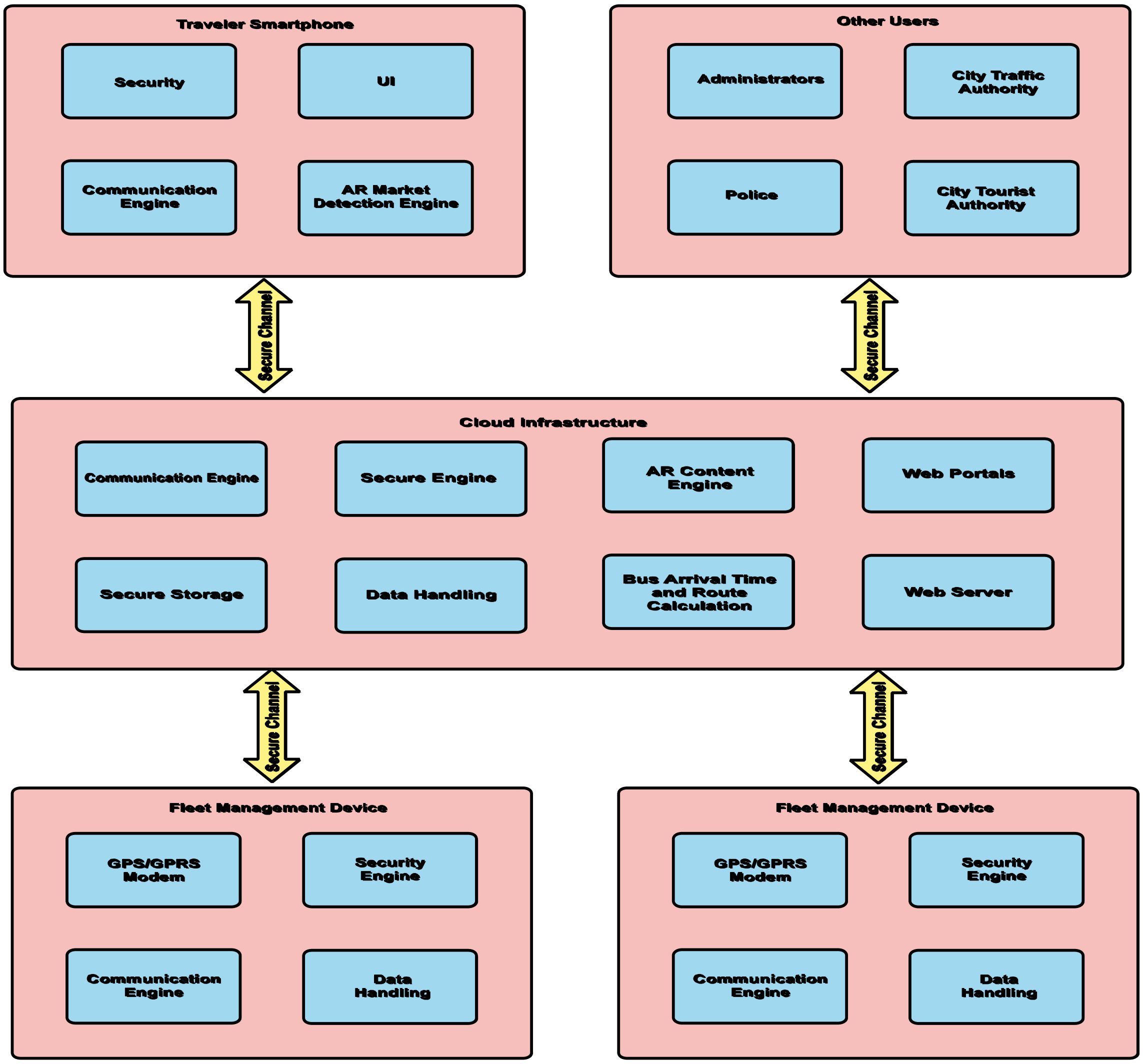

Figure 3: Top level architecture of proposed system.

The system proposed in the paper will generate and handle sensitive data. Hence importance has to be given for security mechanisms which will be implemented in the IOT platform. Travel route and plan specified by passenger's destination location, bus location are all considered sensitive data. These data are generated from fleet management devices. Only authorized users having suitable access mechanisms should be able to access all these sensitive information. Also, the data transfer through communication channels should be done in secure manner without compromising security of public transport infrastructure or privacy aspects of passengers.

A number of studies like [4] [5] [6] address the issue of IOT solutions and architecture implementation and security requirements. Existing security mechanisms can be applied within the IOT architectural stack at various layers, for different purposes some levels and purposes include privacy, protocol and network security, trust, identity management and governance. Various layer of IOT infrastructure need different security mechanisms. The security type required for web applications and data security is different from the security type required for IOT devices.

5. SECURE INFRASTRUCTURE OF IOT

- The following three areas are covered in implementation of security mechanisms for the proposed system:
- Secure storage in cloud infrastructure.
- Privacy of data and accessibility of data for passengers as well as IOT devices.

End to end communication through smart phone and web applications to IOT devices across back-end cloud platform.

Since data handled in the system is very sensitive, its security is of utmost importance []. A Data Processor (DP), a Data Verifier (DV) and a Token Generation (TG) are three main components for a secured storage – generic architecture.

A DP process data and then sends it to the cloud. A Data Verifier checks whether data stored in the cloud is tampered or not. A TG generates tokens which will enable cloud storage provider to retrieve customer data segments. A credential generator is also used in the secure system which implements an access control policy by issuing credentials to different sections of the system. Access control and privacy of data are related to each other [7] and considered in the system proposed in this paper. The public transport company owns the data generated by fleet management devices and only authorized users can access this data. Private data such as travel plans and GPS location will be generated by citizens. Such data are also sensitive and should not be made public. Access to the system by unauthorized fleet management devices should be prevented. To implement all these necessities, access control policies for passengers and IOT devices is established connecting both to the cloud infrastructure at back end.

Standard role-based techniques deployed in standard network infrastructure like LDAP, RADIUS, IPsec and SSH [8] can be used for authorization and access control of citizens, administrators, stakeholders.

The techniques help in identification of the user and then the determination of access privilege is done based on user's role definition within the overall eco-system. In case of IOT devices, role-based access control system are not suitable because individual device identity may not be known may not be important. Hence access control takes place based on criteria like location, proximity etc. Therefore, deployment of mechanism in the proposed system is based upon the scheme of Attribute Based Encryption (ABE) for fine grained access control with no length user authorizing processes involved as described in [9].

In an Attribute Based Encryption system, sets of descriptive attributes are used to label the keys and ciphertext. Here one key can decrypt one particular ciphertext provided a match is found between the key and attributes of the ciphertext. By adopting the above procedure the encrypted and sensitive data can be shared selectively at a fine grained level and multi-level access to various users can be permitted. Associated access rights will also be granted only for the data which the users can use. This technique will be integrated within security framework of the platform and will be incorporated for fleet management devices. Source to Destination communication security will offer confidentiality to the IOT system so that data or messages which are sent to the destination from the source will be hidden from intermediate sections. Suitable encryption and decryption algorithms provide confidentiality inside the IOT system at different levels within the systems architectural stack. Mobile and Web applications are covered by upper layers of the stack. The upper layers thus employ standard security mechanisms like Internet Protocol Security (IPsec) or SSL/TLS which use HTTP protocol. Lower layers of architectural IOT stack use IOT devices IoT devices are generally resource restricted devices. Limited memory, battery life, low CPU processing power, low communication bandwidth hence it imposes certain challenges in case of security implementation. For this reason connection less UDP communication protocol is used for communication between back-end infrastructure and IOT devices. Instead of stream-oriented TCP. Designing of synchronous HTTP in done for TCP and hence it is not possible for UDP –based IOT. Hence, constrained application protocol which is a subset of HTTP will be standardized into a web protocol for IOT [10]

Secure CoAP will make use of datagram transport layer security (DTLS) mandatory to protect sensitive data that is being transmitted as the security protocol for confidential and authenticated communication. Initially DTLS was used for comparably powerful devices that are connected through reliable, high –bandwidth links which is not the usual case. Implementation of searchable encryption method is the aim of the proposed system in which remote storage of encrypted data is done in a distributed system. The owner of these data can perform query operation and still main information confidentiality without allowing external entities to access their data [11] [12].

Cryptographic primitive is the core of security system and can be successfully scaled up or down to offer a variable protection level at the expense of using many or fewer resources. Further, this primitive will be applied at different levels in the architectural stack of proposed system, namely in IOT devices and cloud infrastructure. Light weight cryptography for constrained devices is provided by ISO/IEC 29192 [13].Further optimization of this method can be done to reduce key size and to develop a more efficient algorithm in terms of requirements for computation and also provide a satisfactory security level. The planned approach in particular makes use of curves with key length between 32 and 64 bits as compared to typical 128 bits which leads to short elliptic curves based crypto system [14].Further, the method uses cryptographic primitive signcryption. This will fulfil the task of public encryption and digital signature with low computing and communicating cost compared to "signature then encryption" [15].

CONCLUSION

This paper puts forth the work focused in implementing a novel smart city service within public transportation using augmented reality or AR technology. This service is aimed to be implemented in Bengaluru city which is one of the metropolitan cities in India. Overall system focuses on security aspects to be addressed in the system. Also, focus is made on further enhancements such as ticket purchase in the proposed system. Multi-model transportation can be further implemented and payment for services from buses, trains, cars can be done using on system.

REFERENCE

[1] M. Naphade et al., "Smarter Cities and Their Innovation Challenges," Computer, vol. 44, no. 6, 2011, pp. 32 39.

[2] K. Su, J. Li, and H. Fu, "Smart City and the Applications," Proc. Int'l Conf. Electronics, Comm., and Control (ICECC), 2011, pp. 1028–1031.

[3] C.E.A. Mulligan and M. Olsson, "Architectural Implications of Smart City Business Models: An Evolutionary Perspective," IEEE Comm., vol. 51, no. 6, 2013, pp. 80–85.

[4] Ericsson ConsumerLab, Smart Citizens: How the Internet Facilitates Smart Choices in City Life, Nov. 2014, www. ericsson.com/res/docs/2014/consumerlab/ericsson -consumerlab-smart-citizens.pdf.

[5] X. Sheng et al., "Sensing as a Service: Challenges, Solutions, and Future Directions," IEEE Sensors J., vol. 13, no. 10, 2013, pp. 3733–3741.

[6] B. Guo et al., "From Participatory Sensing to Mobile Crowd Sensing," Proc. IEEE Int'l Conf. Pervasive Computing and Comm. Workshops (PERCOM), 2014, pp. 593–598.

[7] D. Yang et al., "Crowdsourcing to Smartphones: Incentive Mechanism Design for Mobile Phone Sensing," Proc. 18th Int'l Conf. Mobile Computing and Networking (Mobicom), 2012, pp. 173–184.

[8] S. Huangfu et al., "Using the Model of Markets with Intermediaries as an Incentive Scheme for Opportunistic Social Networks," Proc. IEEE 10th Int'l Conf. Ubiquitous Intelligence and Computing and 10th Int'l Conf. Autonomic and Trusted Computing (UIC/ATC), 2013, pp. 142–149.

[9] B. Kantarci and H.T. Mouftah, "Trustworthy Sensing for Public Safety in Cloud-Centric Internet of Things," IEEE Internet of Things J., vol. 1, no. 4, 2014, pp. 360–368.

[10] C. Prandi et al., "Trustworthiness in Crowd-Sensed and Sourced Georeferenced Data," Proc. IEEE Int'l Conf. Pervasive Computing and Comm. Workshops (PERCOM), 2015, pp. 402–407.

[11] B. Kantarci and H.T. Mouftah, "Mobility-Aware Trustworthy Crowdsourcing in Cloud-Centric Internet of Things," Proc. IEEE Int'l Symp. Computers and Communications (ISCC), 2014; doi: 10.1109/ ISCC.2014.6912581.

[12] B. Kantarci and H.T. Mouftah, "Trustworthy Crowdsourcing via Mobile Social Networks," Proc. IEEE Global Comm. Conf. (GLOBECOM), 2014, pp. 2905–2910.

[13] B. Guo et al., "Building Human-Machine Intelligence in Mobile Crowd Sensing," IT Professional, vol. 17, no. 3, 2015, pp. 46–52. 14. B. Kantarci, K.G. Carr, and C.D. Pearsall, "SONATA: Social Network Assisted Trustworthiness Assurance in Smart City Crowdsensing," Int'l J. Distributed Systems and Technologies, vol. 7, no. 1, 2016, pp. 64–84.

[14] Z. Yang et al., "VoteTrust: Leveraging Friend Invitation Graph to Defend Against Social Network Sybils," IEEE Trans. Dependable and Secure Computing, 2015, pp. 1–14.

[15] K. Aihara et al., "Crowdsourced Mobile Sensing for Smarter City Life," Proc. IEEE 7th Int'l Conf. Service-Oriented Computing and Applications (SOCA), 2014, pp.334–337.